Computer Networks

Lecture 6:
Data Link Layer (Cont.)

Local Area Networks
Ethernet

Outline

- LAN addresses and ARP
- Ethernet
- Network devices :Hubs, bridges, switches, gateways, and routers.

Introduction

- LAN provides a path for the transfer, storage, retrieval and distribution of information swiftly between nodes

Objectives of using LANs

- Share files
- Transfer files
- Access information and files
- Share printers or any other device between several workstations

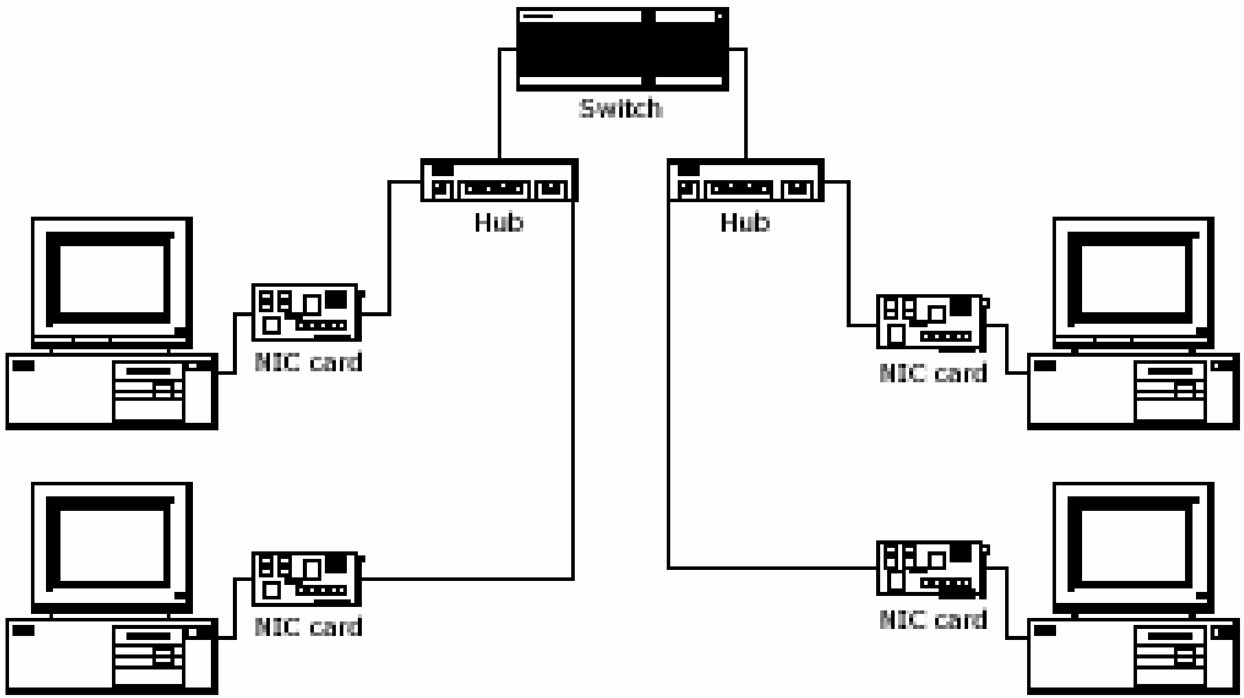
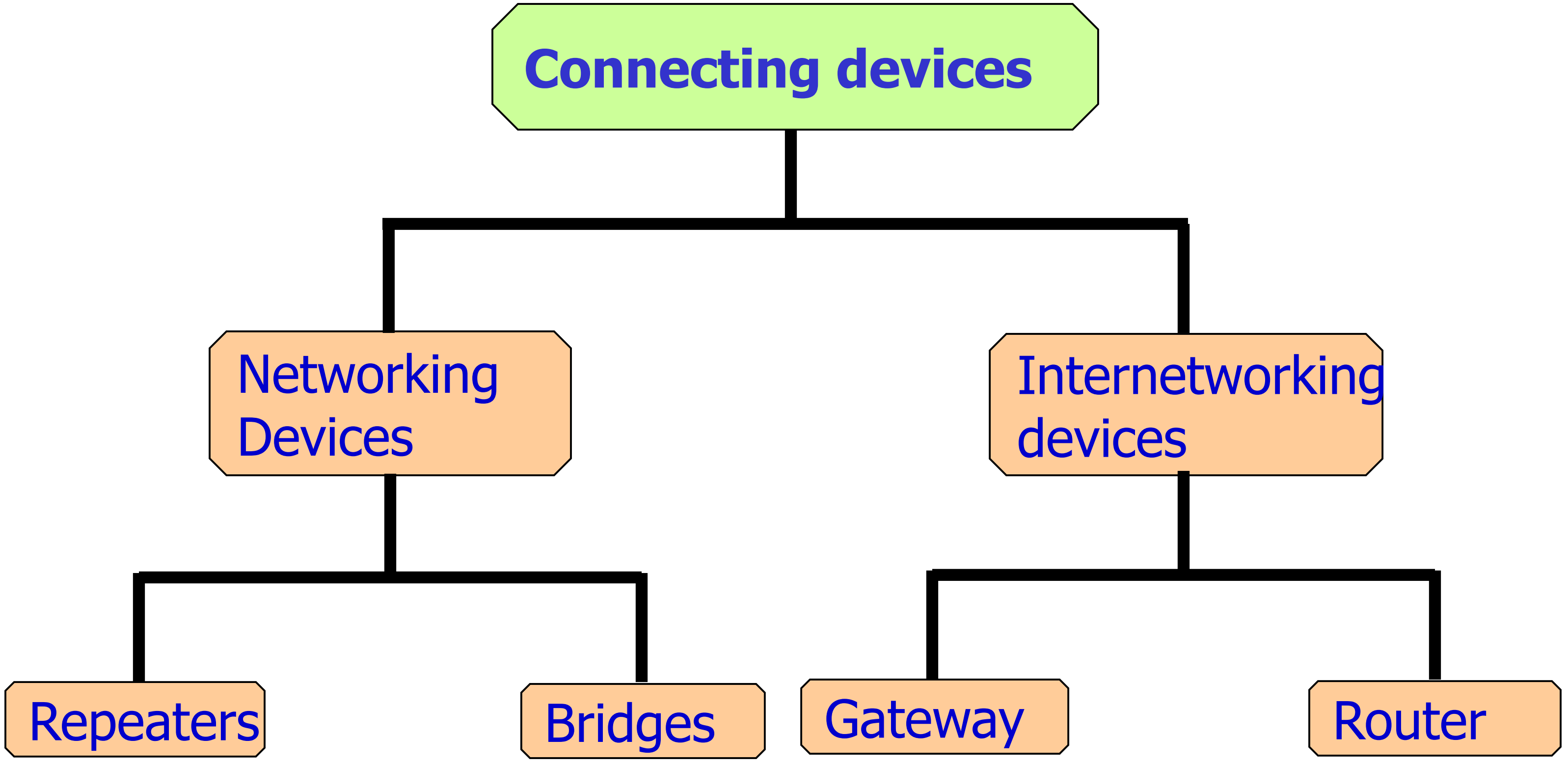


Fig. 4.1: Networking devices.

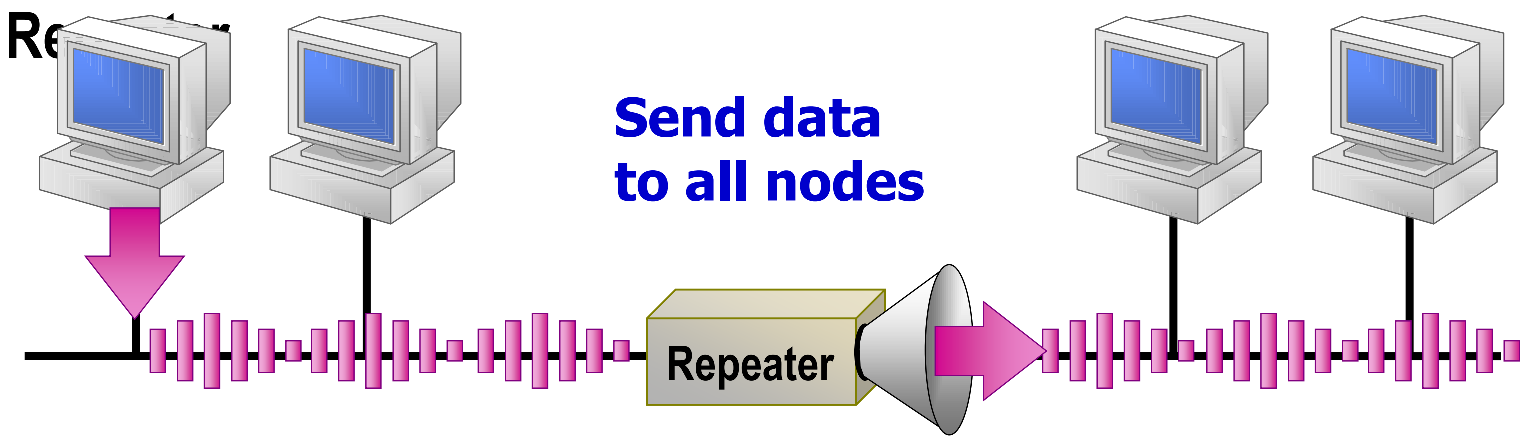
Components of LAN

- Workstation
- File server
- LAN Cable
- LAN adapter (NIC)
  - LANtastic Adapter
  - ARCnet adapter
  - Ethernet adapter
  - Token Ring Adapters
- LAN software
  - Novell Netware
  - OS/2 LAN server and LAN manager
  - LANtastic
  - Netware Lite
  - Windows family
  - Linux
  - Mac OS


Connecting devices
Networking Devices
Internetworking devices
Repeaters
Bridges
Gateway
Router

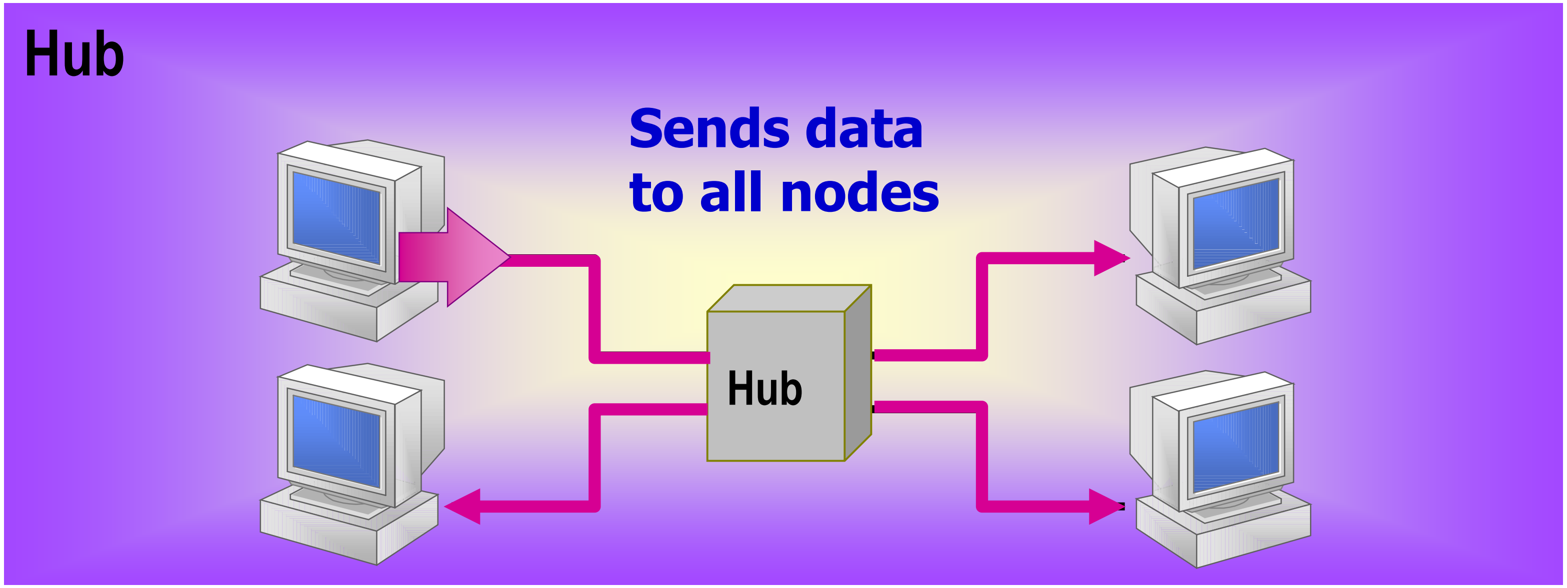
Repeater

- A repeater connects segments of a LAN.
- It forwards every frame; it has no filtering capability.
- It is a regenerator; not an amplifier.



Hub

- It is a multiport repeater.
- It is used to create connections between stations in a physical star topology.
- It receives the message on one port and retransmits it on all ports.

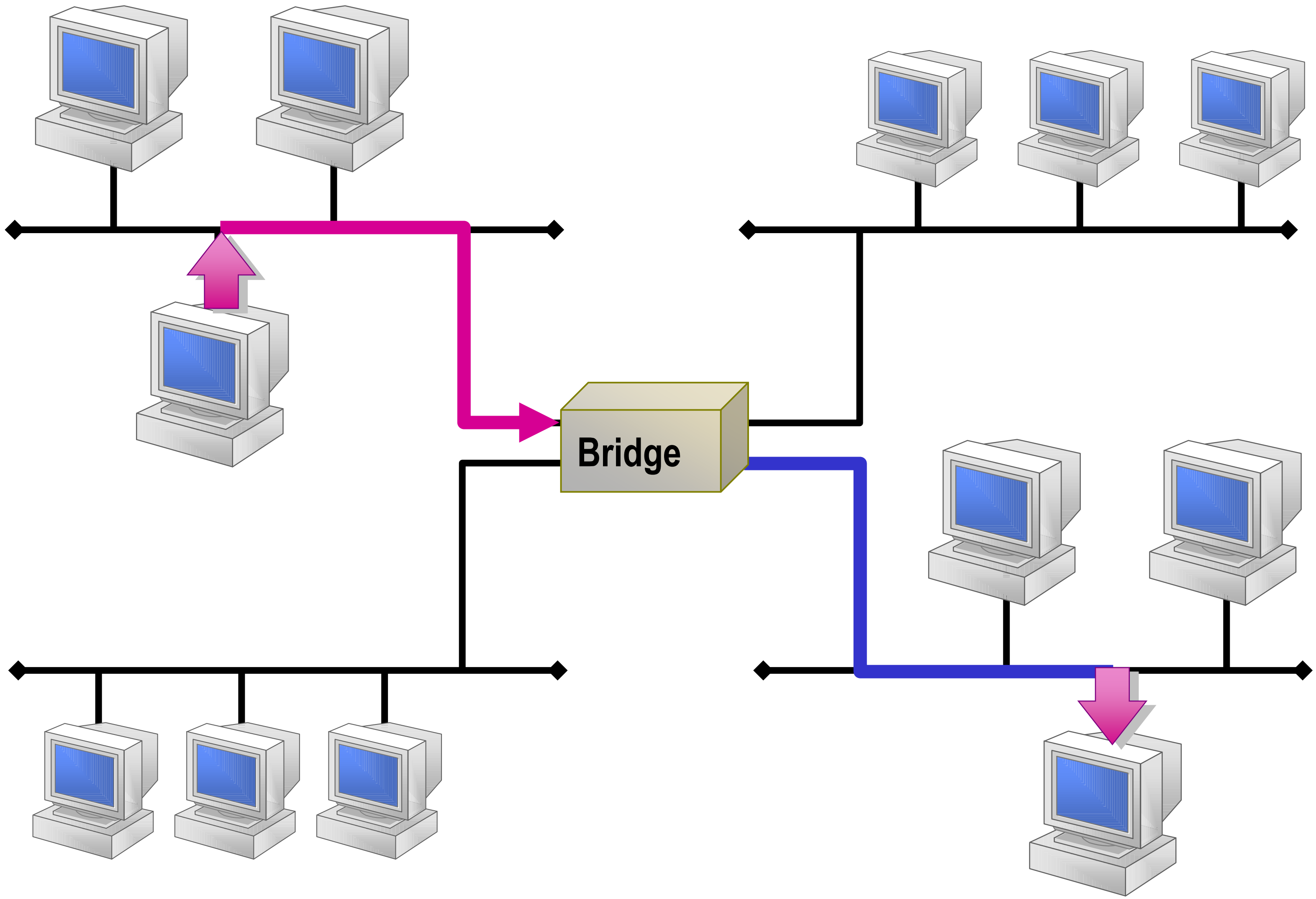


- **Repeater** and **Hub** are layer 1 devices.
- Repeater address the issue of attenuation. Attenuation is the loss of signal over distance. Repeater rebuilt the electrical signal that comes in and send it out to other side.
- Hub is a multi-port repeater. Electrical signal came into any one hub port will be repeated on all other ports.
- The layer 1 devices are dumb, they have no decision making abilities. Hubs do not read any of the data passing through them, and they are not aware of the source or destination of the frame.
- All the devices attached to a hub are belong to one collision domain, which means if two hosts try to send data at the same time, a collision will occur.
- All the devices attached to a hub are also belong to one broadcast domain, that is, broadcast frame sent by one host will be received by all other hosts in the network.

Bridge

- It has a table used in filtering decisions.
- It does not change the physical MAC address in a frame.
- It can divide a large network into smaller segments.
- It regenerates the signal, checks the address of destination and forwards it only to the segment to which this address belongs.
- It cannot translate between protocols.

Bridge



Bridges

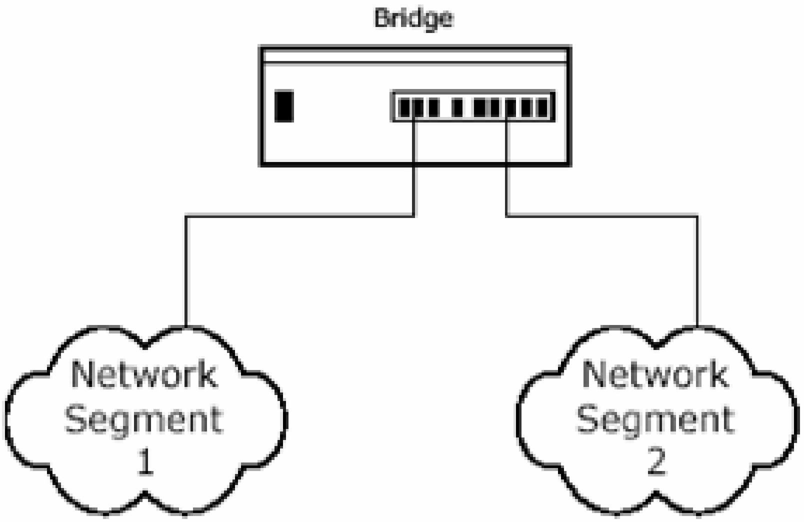


Fig. 4.10: Bridge connecting network segments.

- **Bridge and Switch are layer 2 devices**. They can make decisions about to which port the frames will go, based on MAC Addresses. Bridges and switches help avoid frame collision by breaking down one collision domain to two or more smaller collision domains, then buffer and forward frames between them. Nowadays, a switch can be configured to allow each connected host to have its own individual collision domain. As a result, all the hosts can trasnmit data simultaneously without collision, because they no longer share the bandwidth with each other. It is important to notice hosts attached to bridge or switch still belong to the same broadcast domain.

Switches

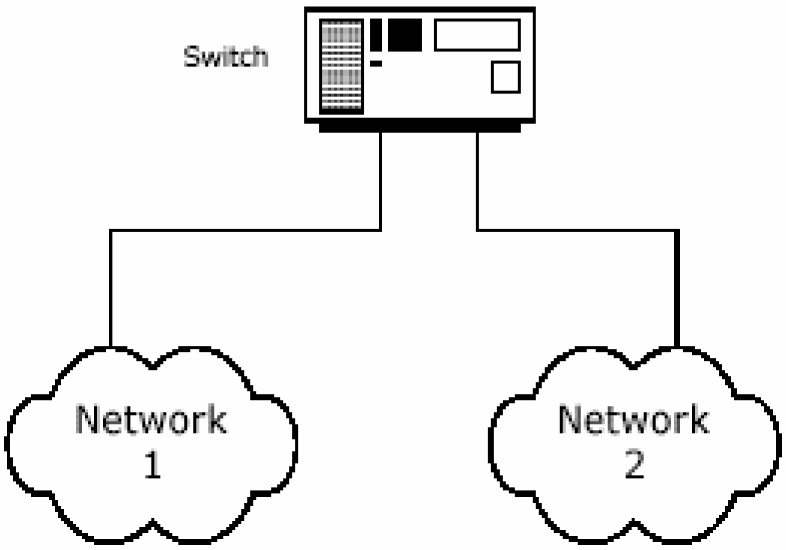


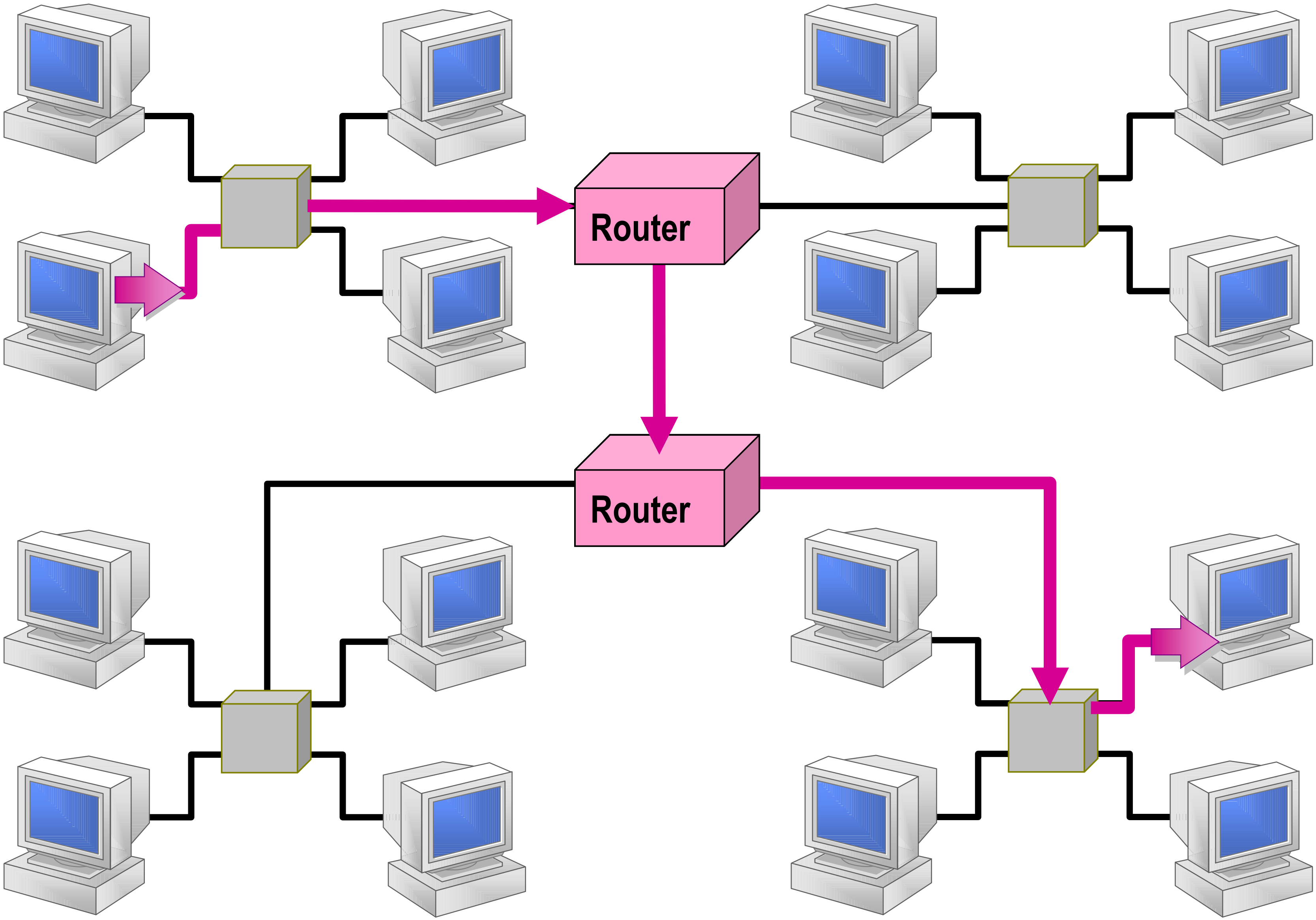
Fig. 4.12: Switch connecting networks.

Router

- It has access to network layer address and determines the best path for a particular transmission.
- It can relay packets among multiple interconnected networks.
- It transfers, accepts and relays packets only across networks using similar protocols.

- **Router** is layer 3 device.. Router maintains a routing table. The purpose of router is to route packets from one broadcast domain to anotherThe routing table contains ip addresses associated with interfaces, out of which the packet will be forward to.

Router



Routers

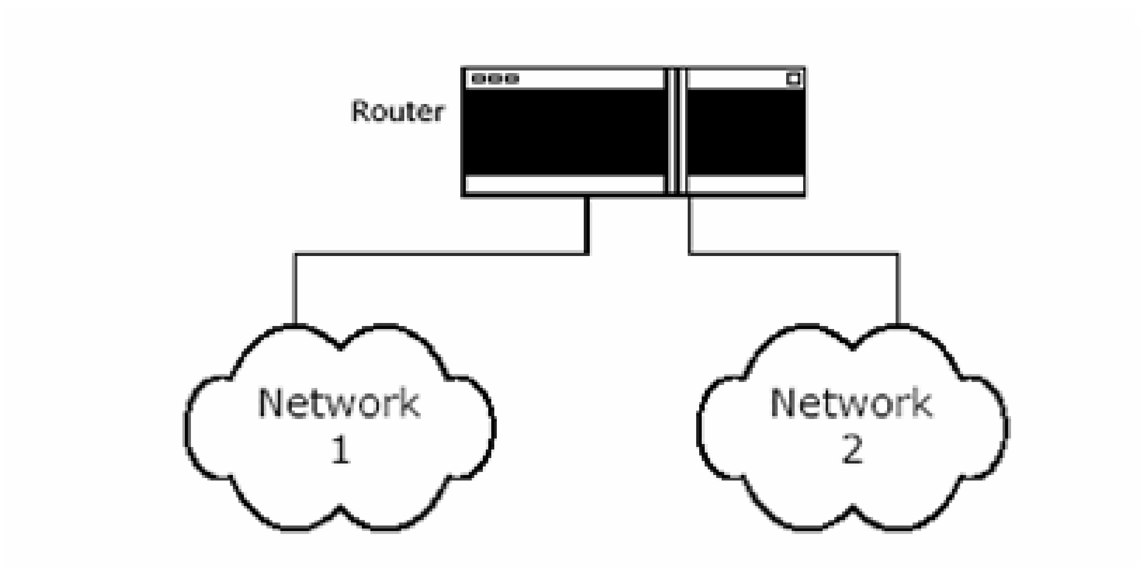


Fig. 4.11: Router connecting networks.

- **Collision Domains** – A collision domain is defined as a network segment that shares bandwidth with all other devices on the same network segment. Generally speaking, A Collision Domain includes all of the Ethernet segments between a pair of bridges or other layer 2 devices. When two hosts on the same network segment transmit at the same time, the resulting digital signals will fragment or collide, hence the term collision domain.
- **Broadcast Domain** – A broadcast domain is defined as all devices on a network segment that hear broadcasts sent on that segment.

- All devices plugged into a **hub** are in the same collision domain and the same broadcast domain.
- All devices plugged into a **switch** are in separate collision domains but the same broadcast domain. Although, you can buy special hardware to break up broadcast domains in a switch, or use a switch capable of creating VLANs. VLANs breakup broadcast domains.
- **Hubs** and **Repeaters** extend collision and broadcast domains.
- **Switches**, **Bridges** and **Routers** break up collision domains.
- **Routers** (and **Switches using VLANs**) break up broadcast domains.

Bridging vs. LAN Switching

- Layer 2 switches are just bridges with a lot more ports, more advanced functionality, and higher speed. They both forward layer 2 broadcasts, learn MAC addresses by examining the source address of each frame received and make forwarding decisions based on layer 2 addresses.

Gateway

- It operates in all 7 layers of OSI model.
- It is a protocol converter.
- It can accept a packet formatted for one protocol (Appletalk) and convert it to a packet formatted for another protocol (TCP/IP) before forwarding it.
- It is generally software installed within a router

Gateways

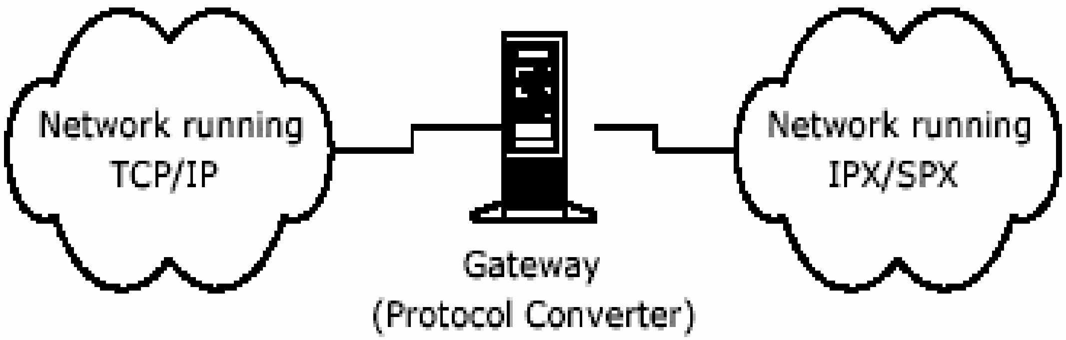
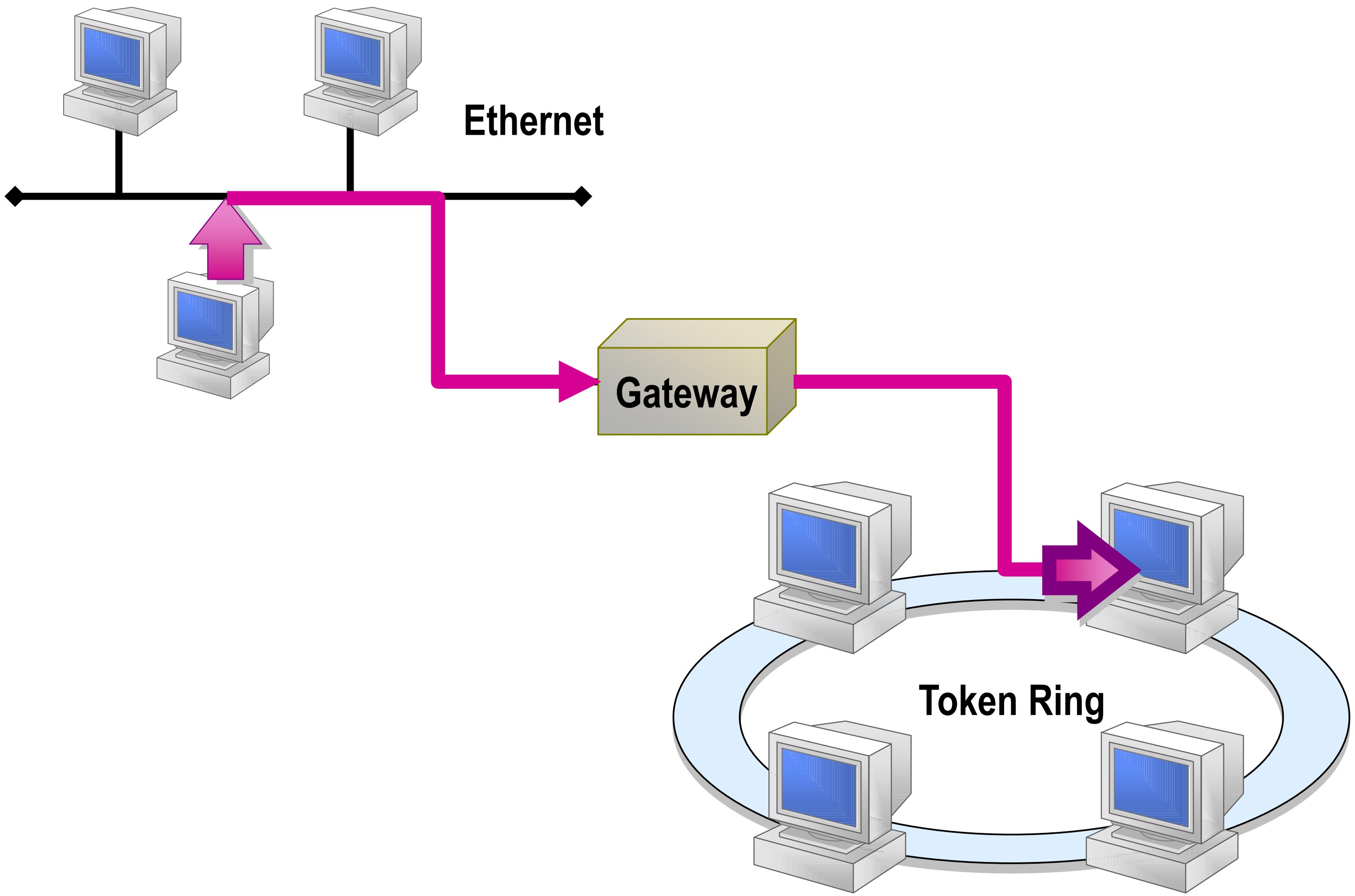


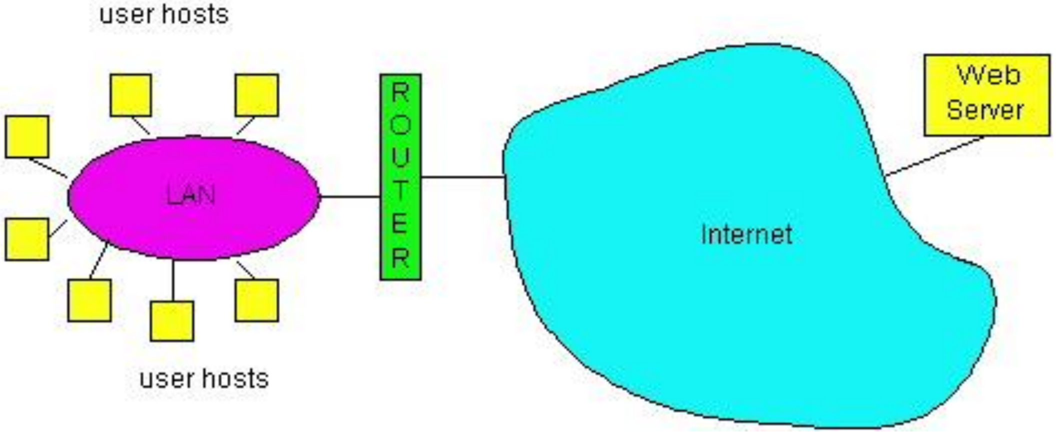
Fig. 4.13: Gateway operation.

Gateway



LAN technologies

- Addressing
- Ethernet
- hubs, bridges, switches
- 802.11
- PPP
- ATM



LAN Addresses

32-bit IP address:

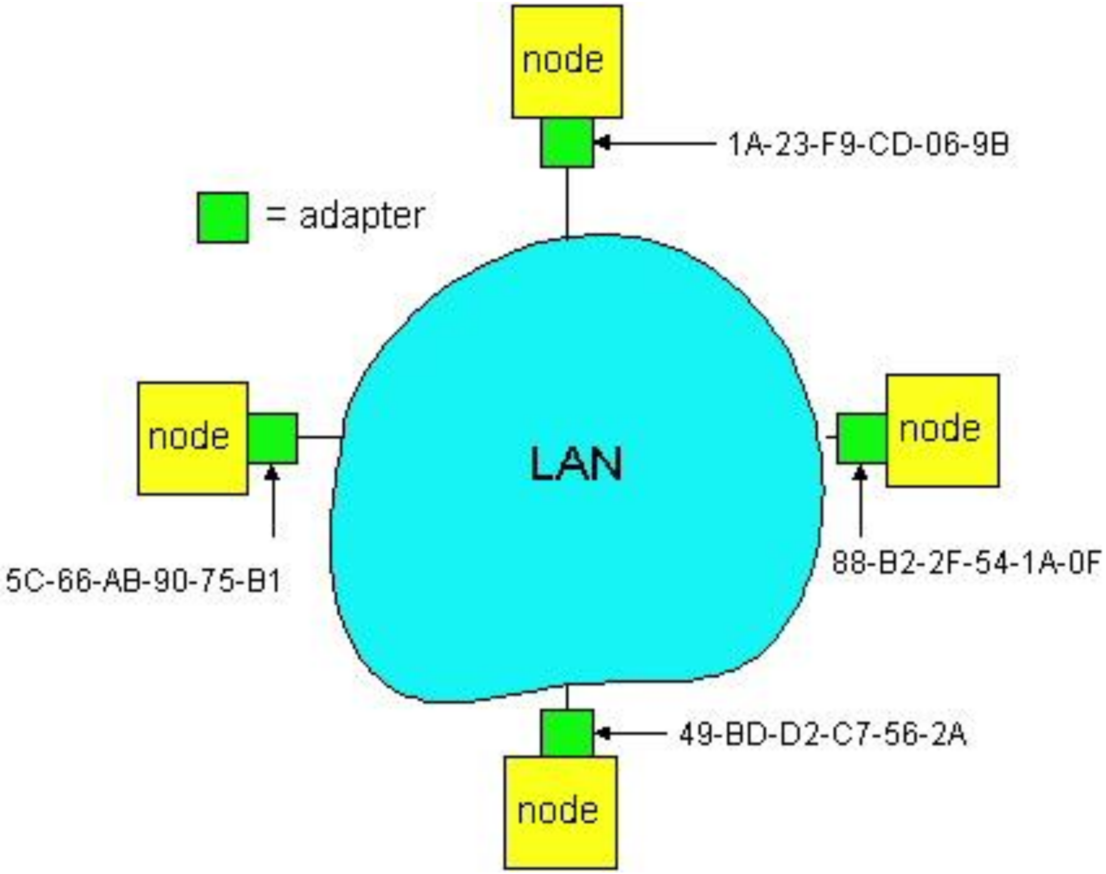
- *network-layer* address
- used to get datagram to destination IP network (recall IP network definition)

LAN (or MAC or physical or Ethernet) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48 bit MAC address (for most LANs) burned in the adapter ROM

LAN Addresses

Each adapter on LAN has unique LAN address



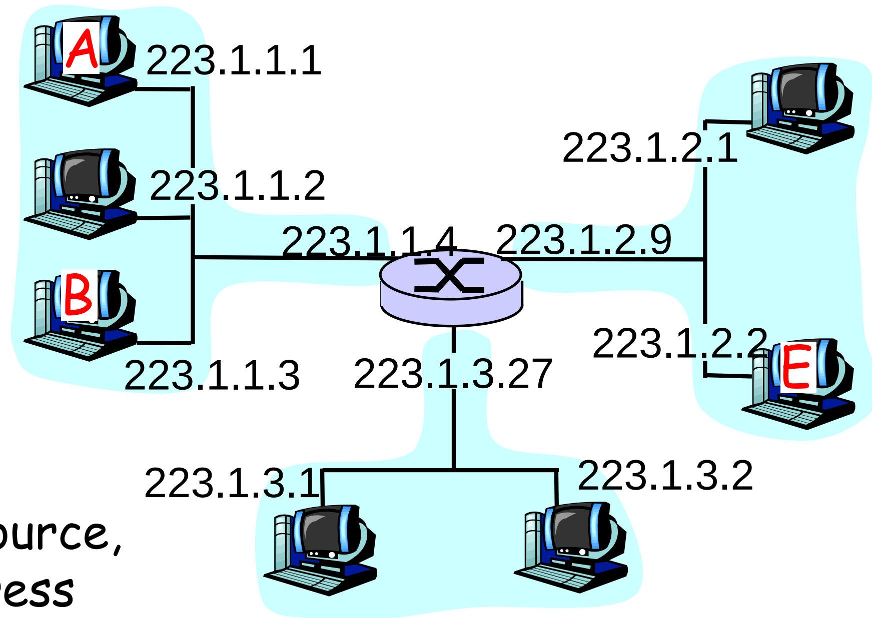
LAN Address (more)

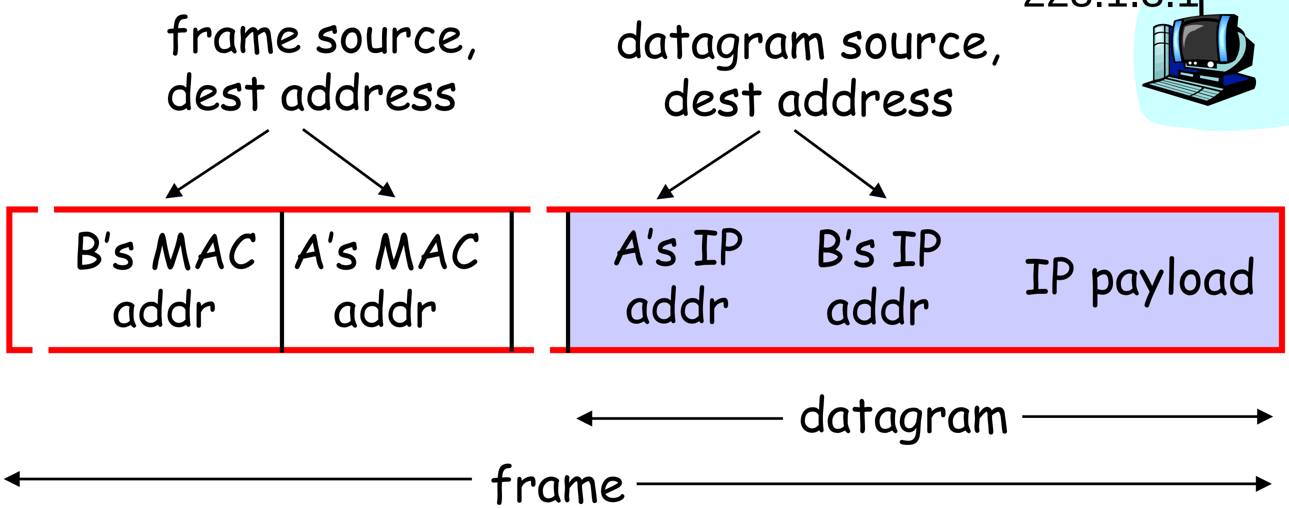
- MAC address allocation administered by IEEE
- A manufacturer (Dlink, 3Com, Cisco…) buys portion of MAC address space (to assure uniqueness)
  - First 24 bits : identifies manufacturer
  - Last 24 bits: with one manufacturer

Recall earlier routing discussion

Starting at A, given IP datagram addressed to B:

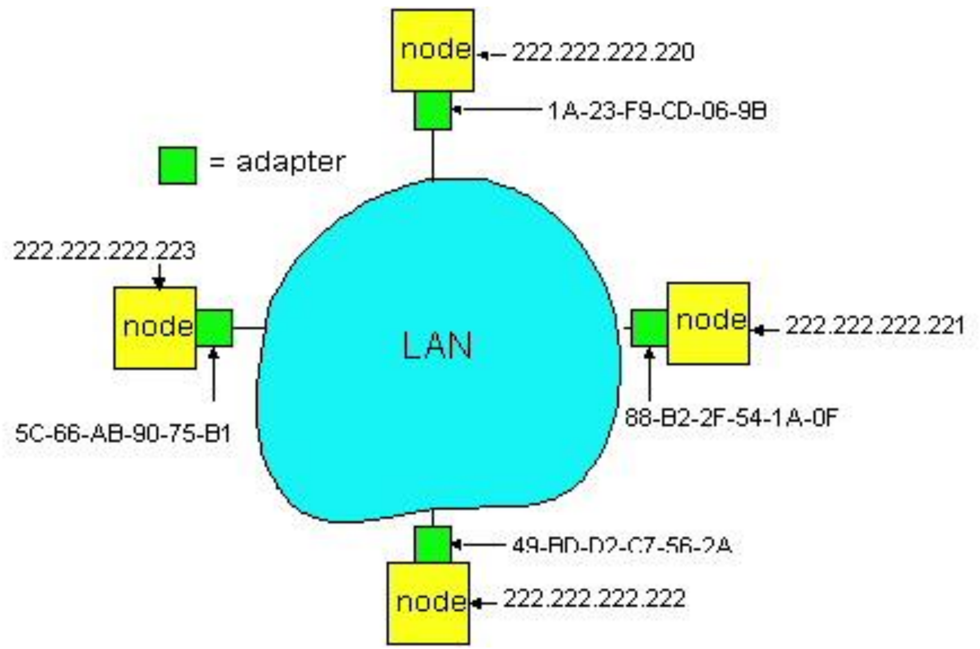
- look up net. address of B, find B on same net. as A
- link layer send datagram to B inside link-layer frame





ARP: Address Resolution Protocol

Question: how to determine MAC address of B knowing B's IP address?



- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

ARP protocol

- A wants to send datagram to B, and A knows B's IP address.
- Suppose B's MAC address is not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - all machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
- ARP is "plug-and-play":
  - nodes create their ARP tables without intervention from net administrator

Broadcast addr: FF-FF-FF-FF-FF-FF

Outline

- LAN addresses and ARP
- Ethernet
- Hubs, bridges, and switches
- Wireless links and LANs
- PPP
- ATM

Ethernet

"dominant" LAN technology:

- cheap - 100Mbs.
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps

Ethernet LAN

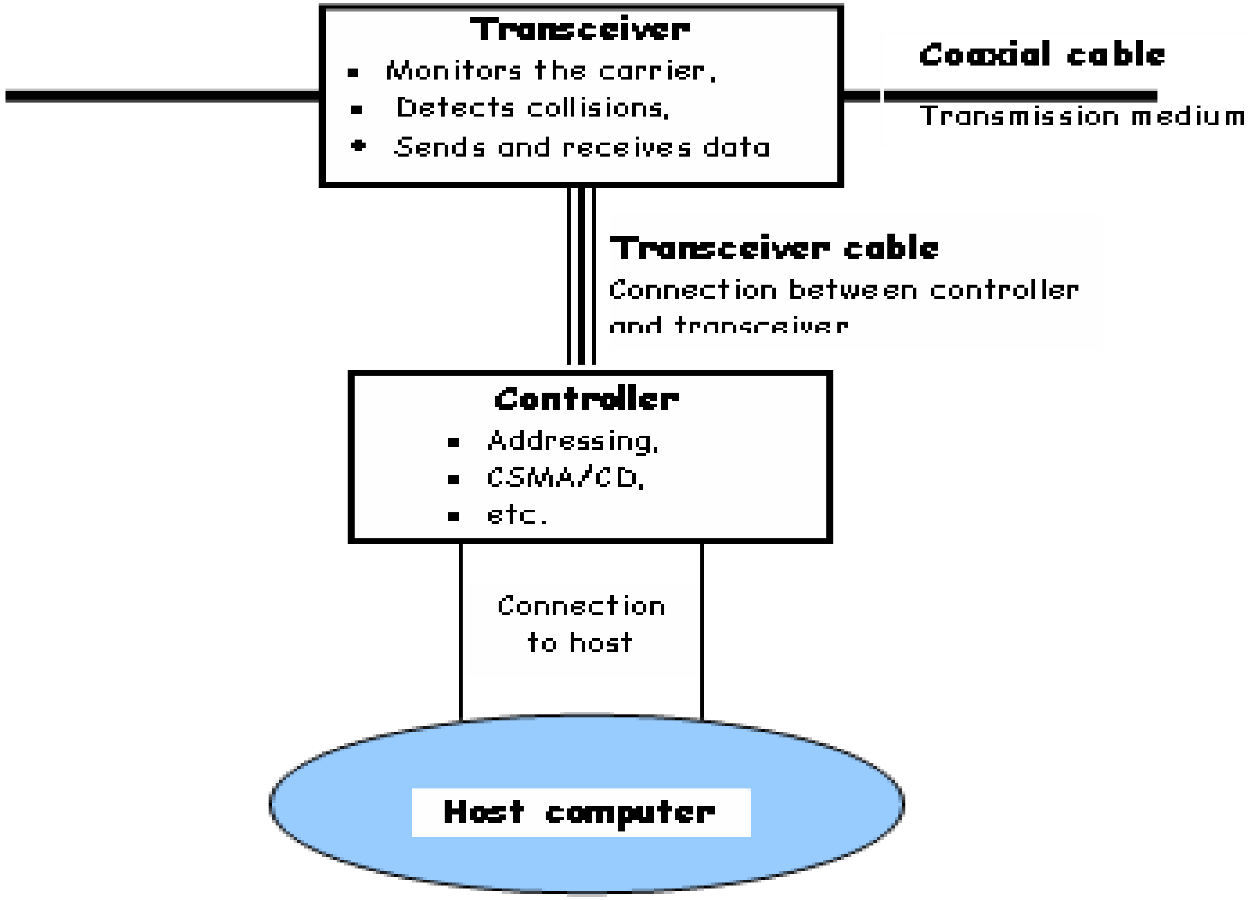
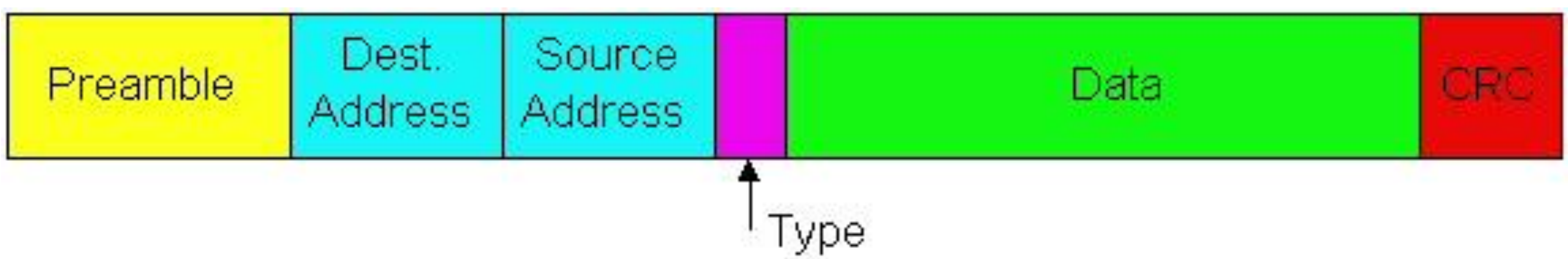


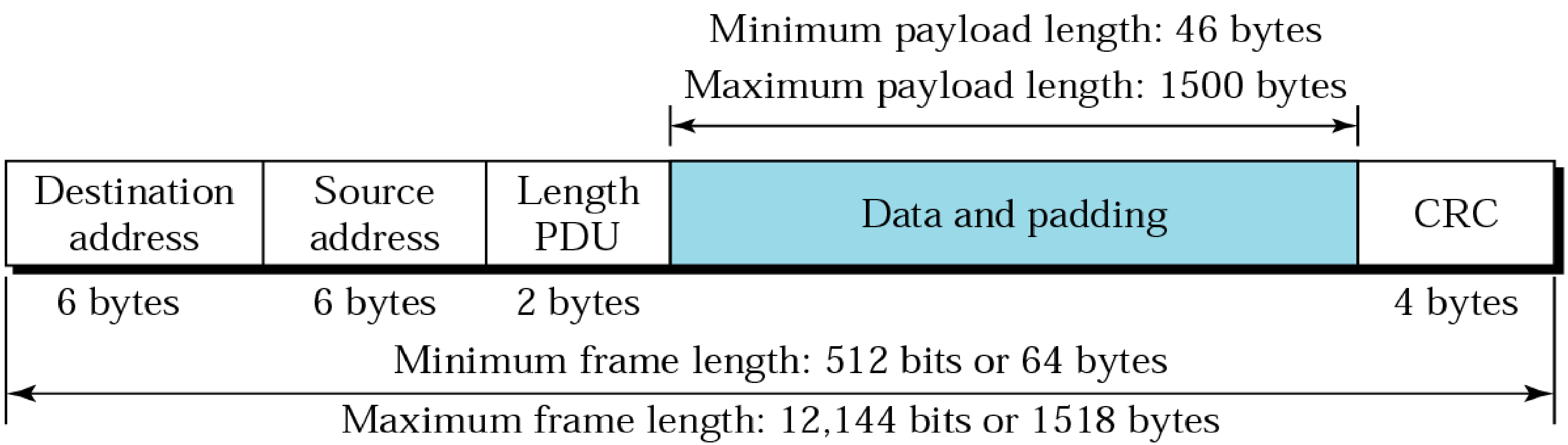
Fig. 4.14: Ethernet components.

Ethernet Frame Structure (more)

- Type: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: checked at receiver, if error is detected, the frame is simply dropped



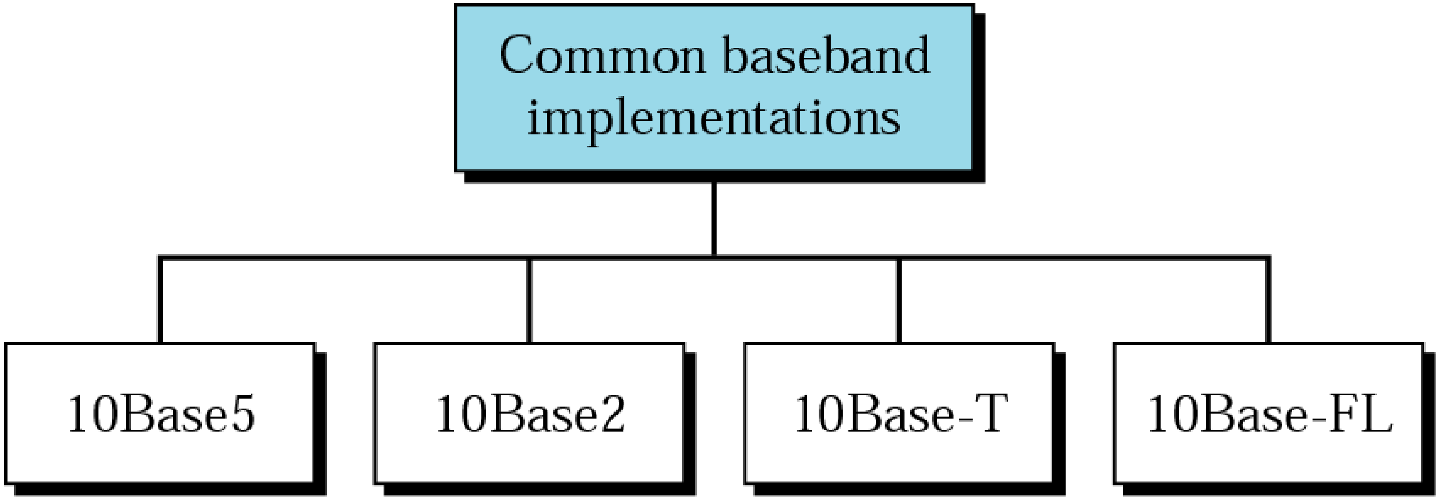
Frame Size


Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

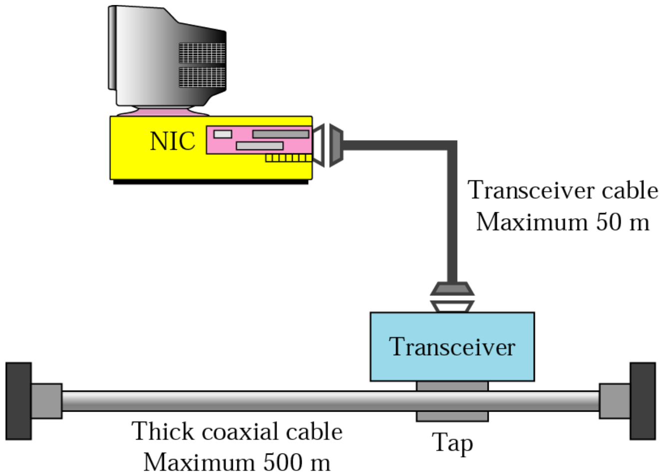
Ethernet uses CSMA/CD

- No slots
- adapter doesn't transmit if it senses that some other adapter is transmitting, that is, carrier sense
- transmitting adapter aborts when it senses that another adapter is transmitting, that is, collision detection
- Before attempting a retransmission, adapter waits a random time, that is, random access

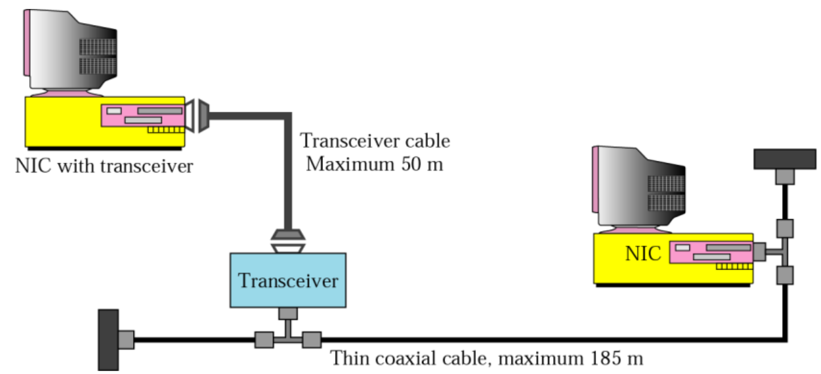
Implementation of Traditional Ethernet



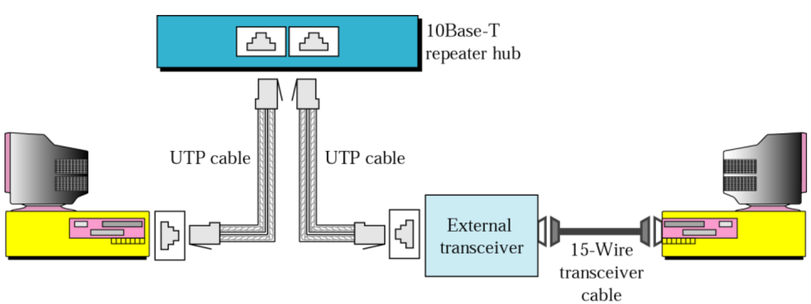
Traditional Ethernet: Implementation



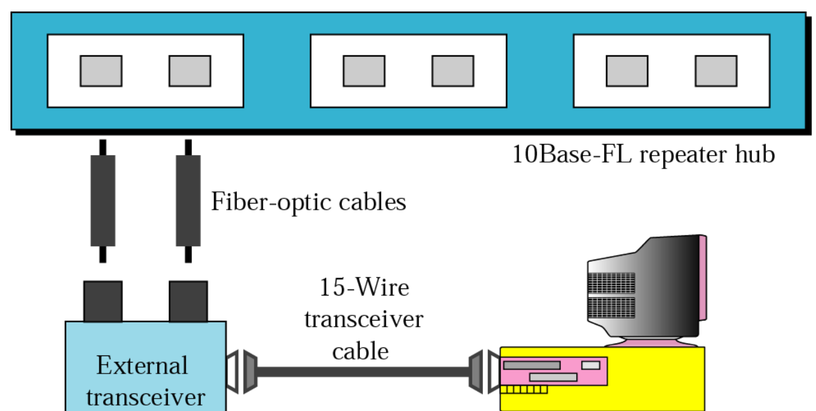
10Base-5 (thicknet)



10Base-2 (cheapernet)



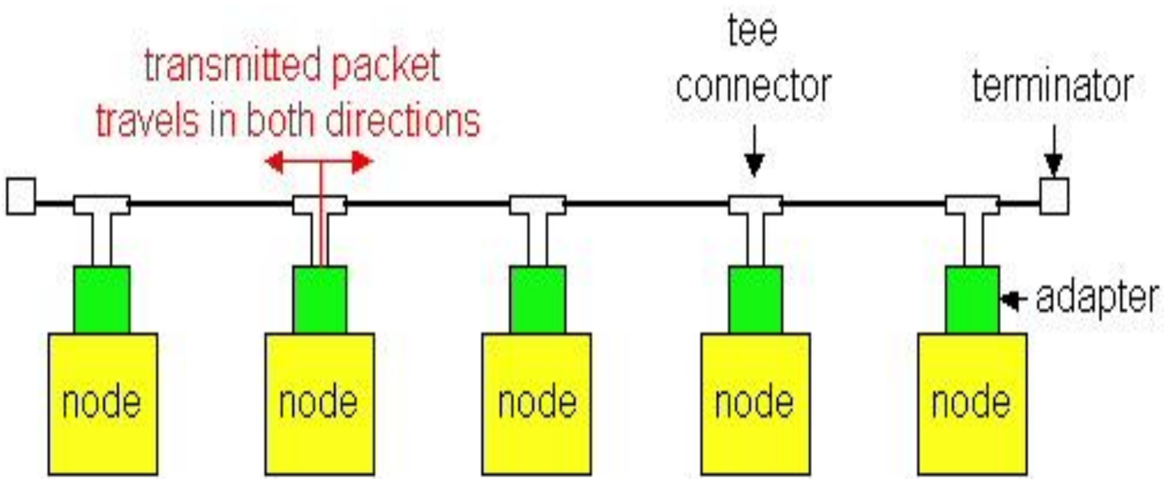
10Base-T



10Base-FL(fiber-link)

Ethernet Technologies: 10Base2

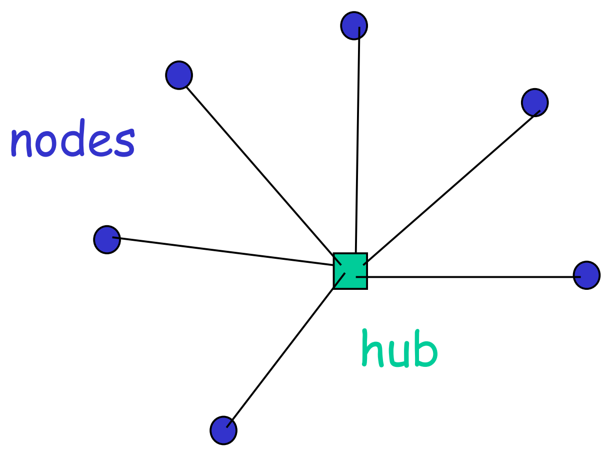
- 10: 10Mbps; 2: under 200 meters max cable length
- thin coaxial cable in a bus topology



- repeaters used to connect up to multiple segments
- repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!
- has become a legacy technology

10BaseT and 100BaseT

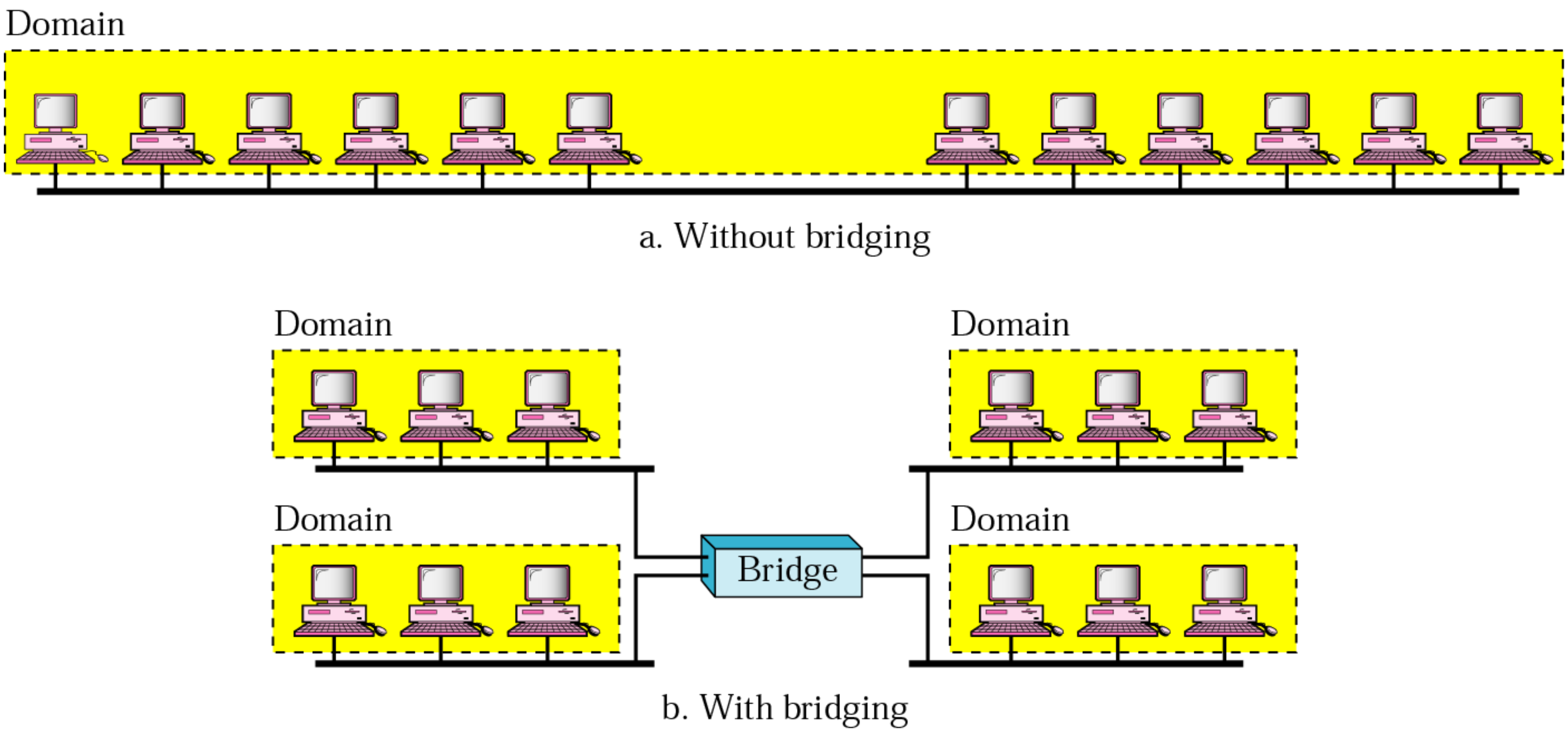
- 10/100 Mbps rate; latter called "fast ethernet"
- T stands for Twisted Pair.
- Nodes connect to a hub: "star topology"; 100 m max distance between nodes and hub



Outline

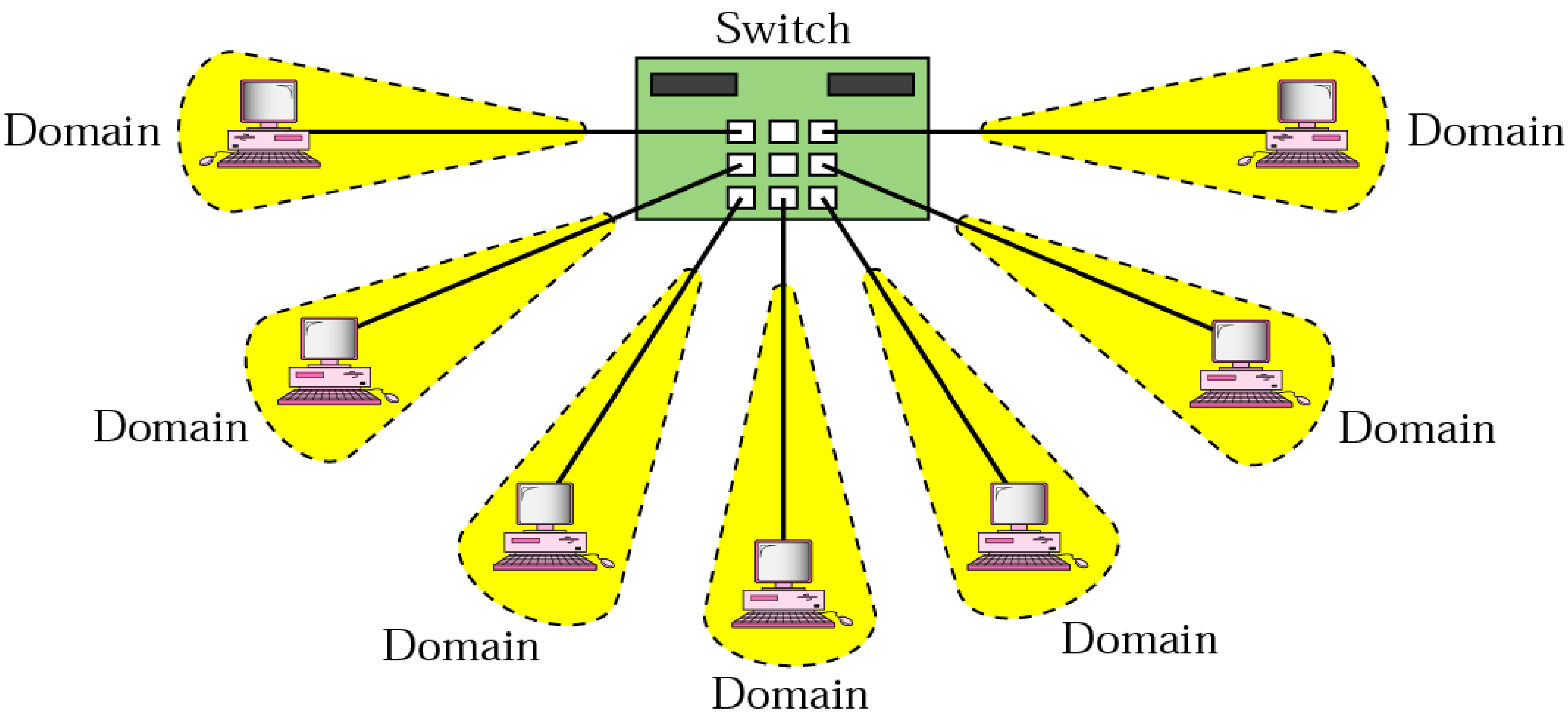
- LAN addresses and ARP
- Ethernet
- Network devices :Hubs, bridges, switches, routers and gateways.

Bridged Ethernet



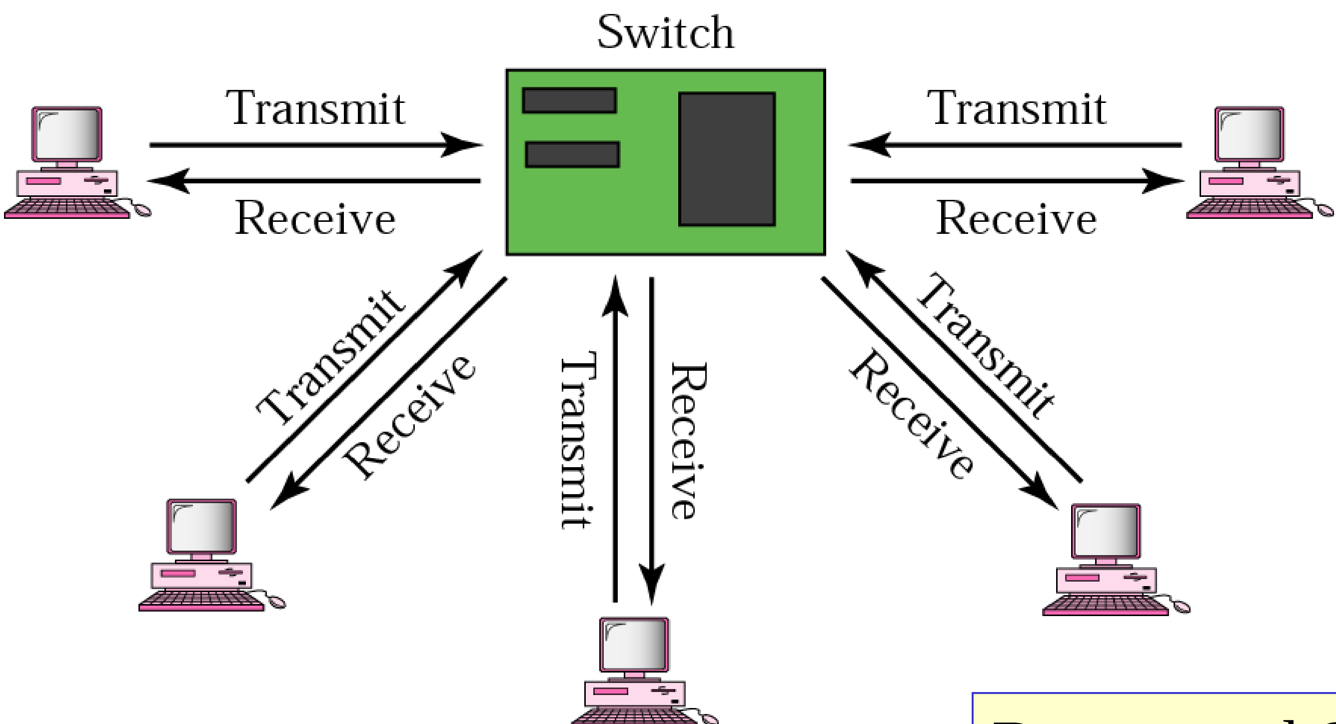
Collision separation-increase bandwidth

Switched Ethernet



Only station and switch share the bandwidth => 5Mbps each

Full-duplex Switched Ethernet



Do we need CSMA/CD?

10Base-2, 10Base-5: half-duplex

10Base-T: full duplex

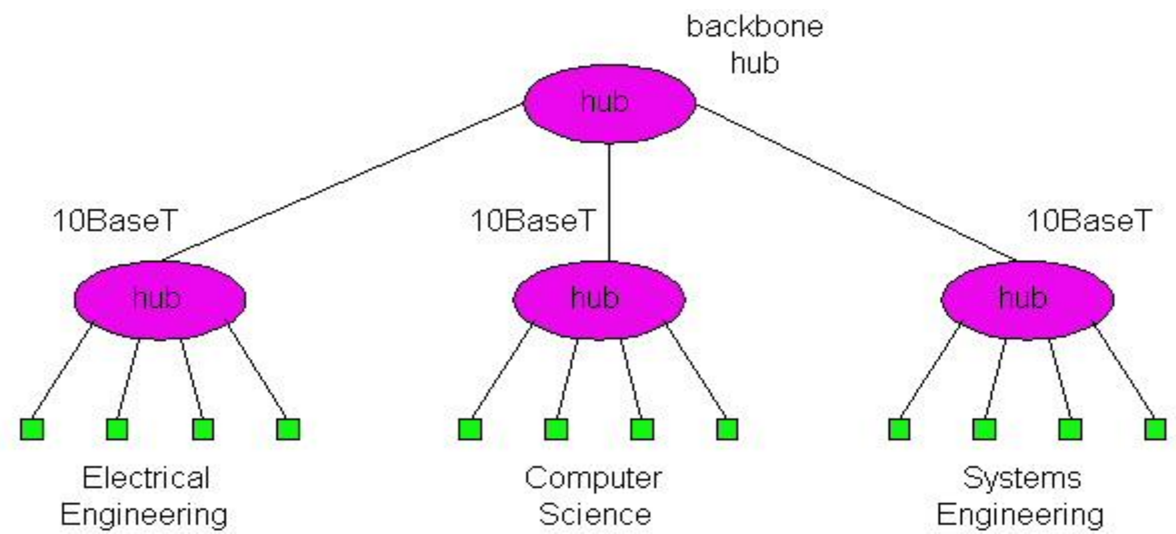
MAC control is added to provide flow/error control

Interconnecting LAN segments

- Hubs
- Bridges
- Switches
  - Remark: switches are essentially multi-port bridges.
  - What we say about bridges also holds for switches!

Interconnecting with hubs

- Backbone hub interconnects LAN segments
- Extends max distance between nodes
- But individual segment collision domains become one large collision domain
  - if a node in CS and a node EE transmit at same time: collision
- Can't interconnect 10BaseT & 100BaseT

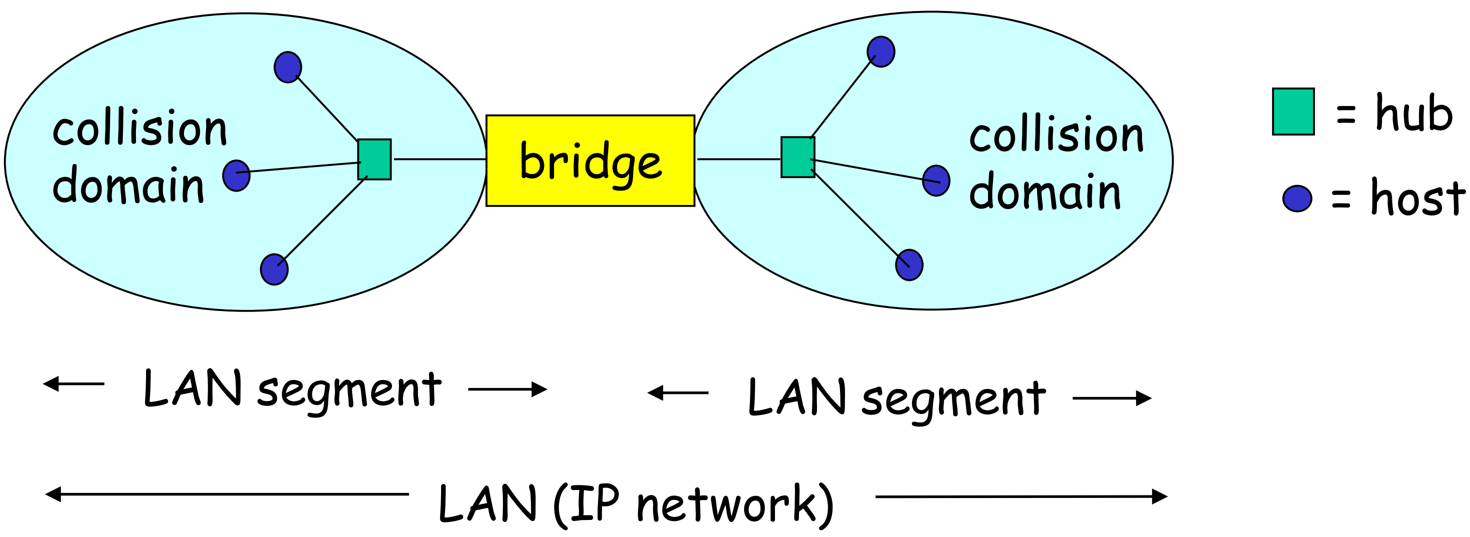


Bridges

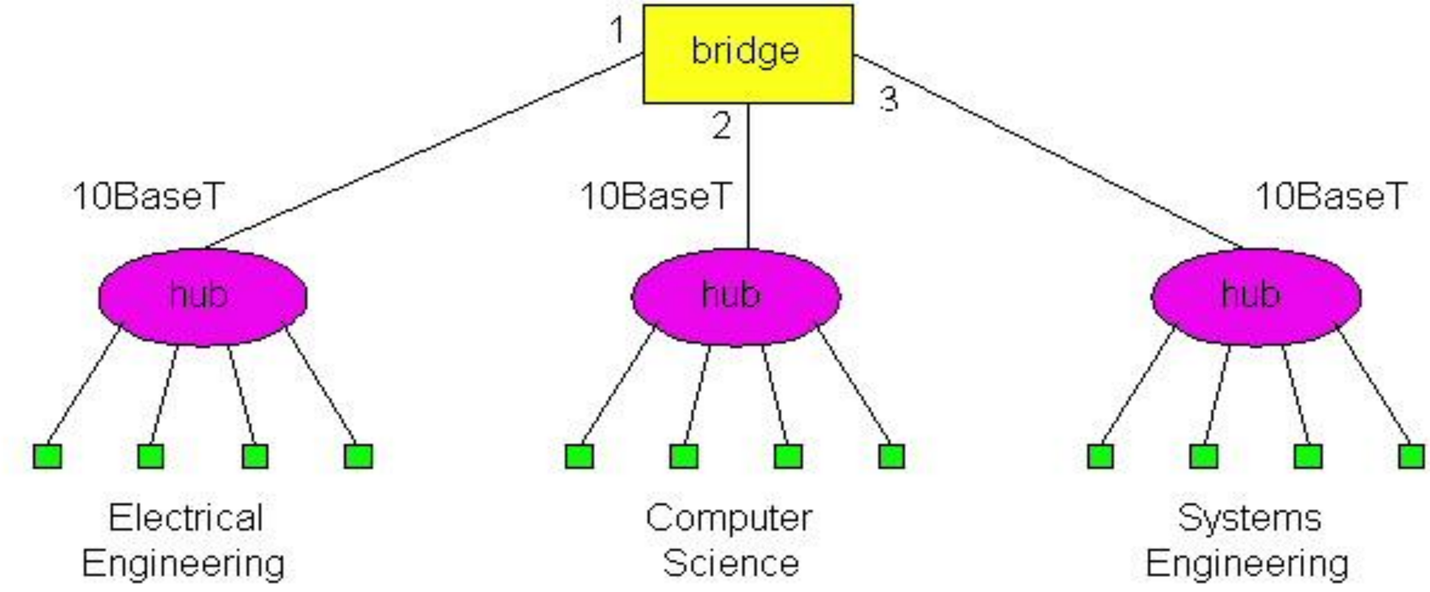
- Link layer device
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC dest address
  - when frame is to be forwarded on segment, uses CSMA/CD to access segment
- plug-and-play, self-learning
  - bridges do not need to be configured

Bridges: traffic isolation

- Bridge installation breaks LAN into LAN segments
- bridges filter frames:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



Forwarding



How do determine to which LAN segment to forward frame?

- Looks like a routing problem...

Self learning

- A bridge has a bridge table
- bridges *learn* which hosts can be reached through which interfaces
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender/location pair in bridge table

Filtering/Forwarding

When bridge receives a frame:

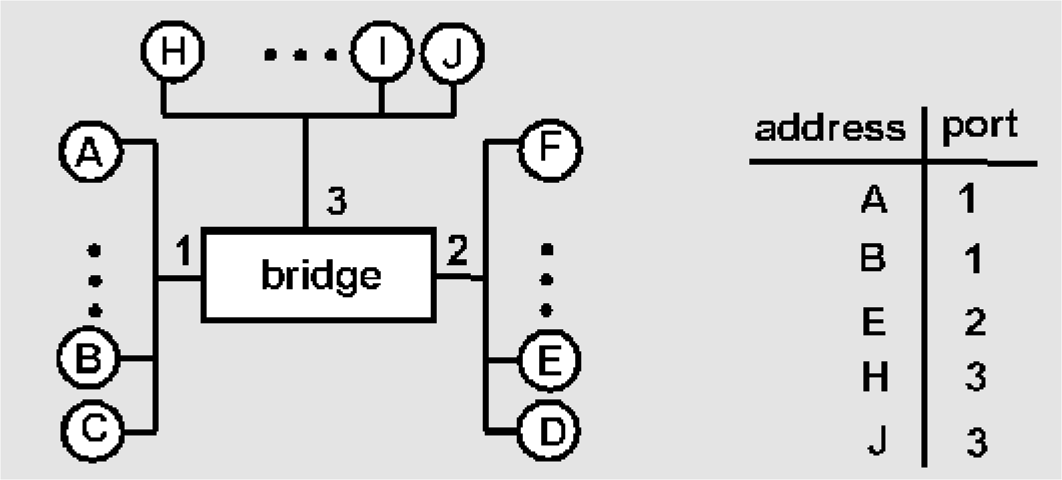
index bridge table using MAC dest address

if entry found for destination
    then{
        if dest on segment from which frame arrived
            then drop the frame
            else forward the frame on interface indicated
        }
    else flood

forward on all but the interface on which the frame arrived

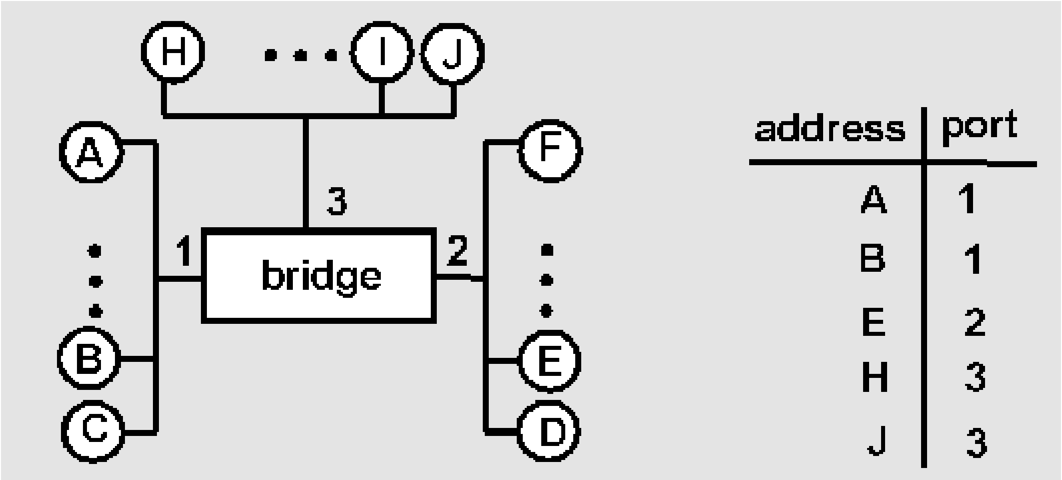
Bridge example

Suppose C sends frame to D and D replies back with frame to C.



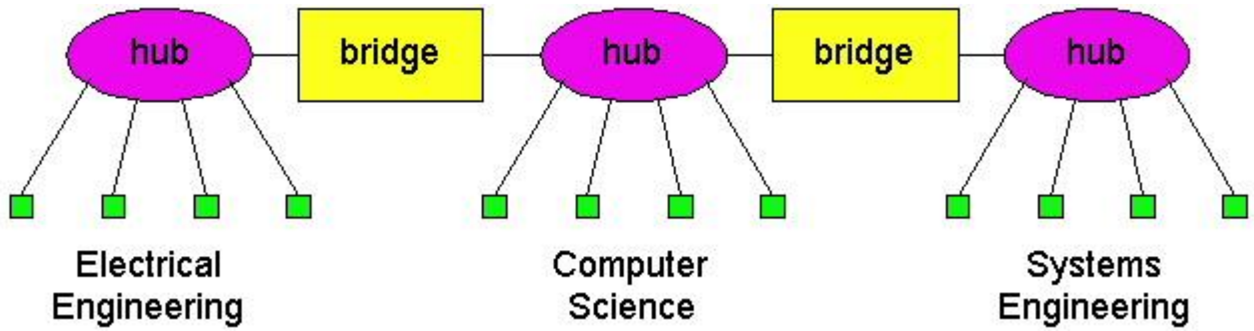
- Bridge receives frame from C
  - notes in bridge table that C is on interface 1
  - because D is not in table, bridge sends frame into interfaces 2 and 3
- frame received by D

Bridge Learning: example



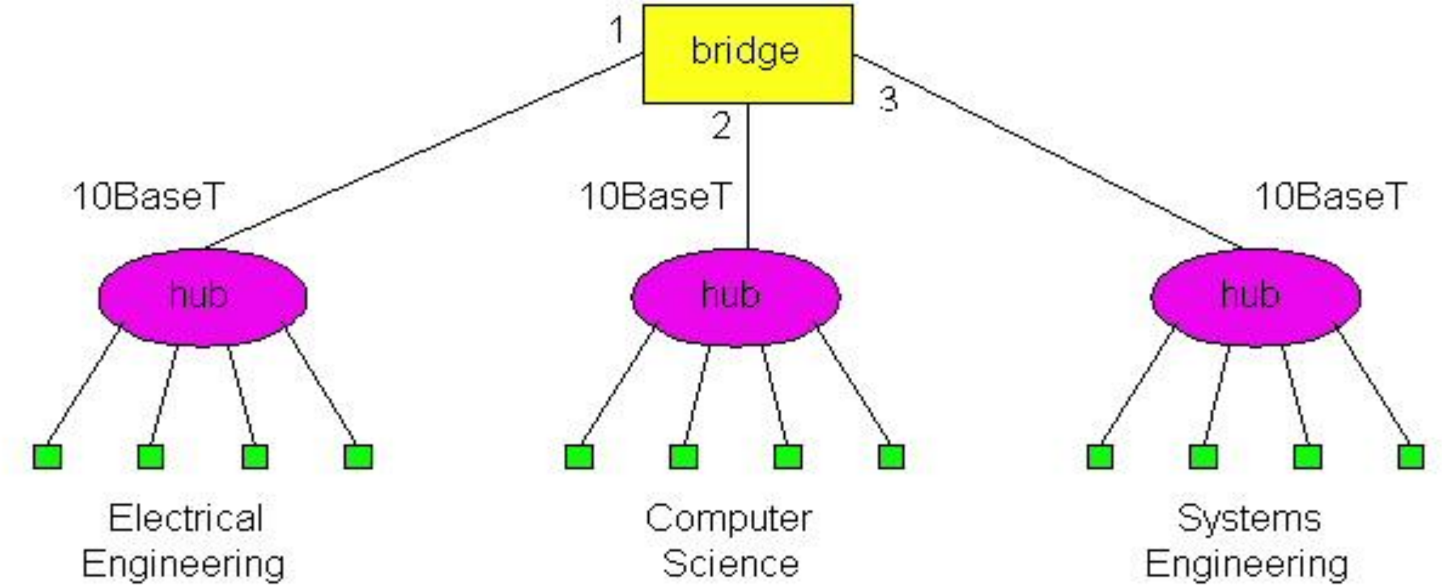
- D generates frame for C, sends
- bridge receives frame
  - notes in bridge table that D is on interface 2
  - bridge knows C is on interface 1, so *selectively* forwards frame to interface 1

Interconnection without backbone



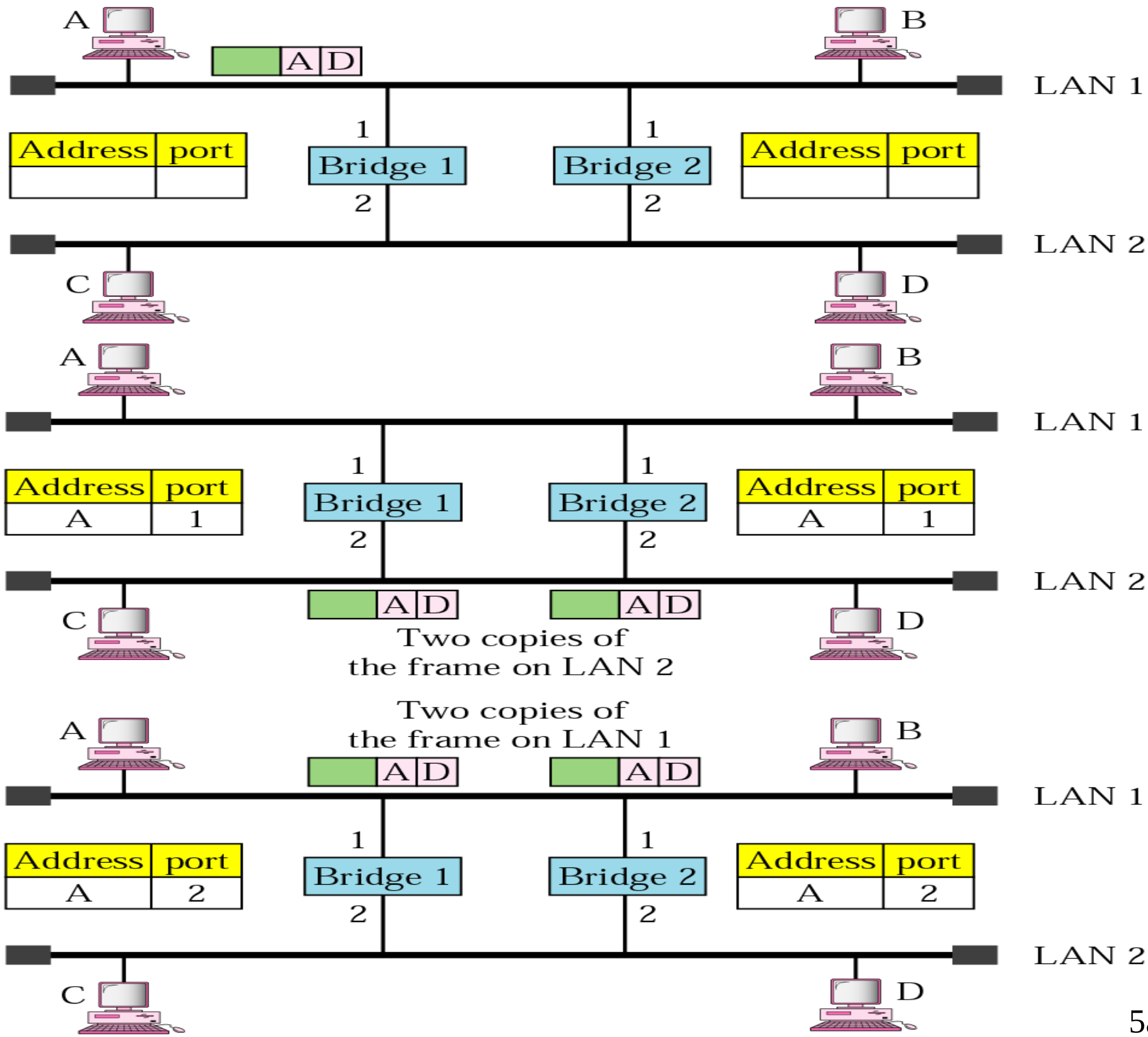
- Not recommended for two reasons:
  - single point of failure at Computer Science hub
  - all traffic between EE and SE must path over CS segment

Backbone configuration



Recommended !

Loop Problem



a. Station A sends a frame to station D

b. Both bridges forward the frame and improve tables

c. Both bridges forward the frame and improve tables

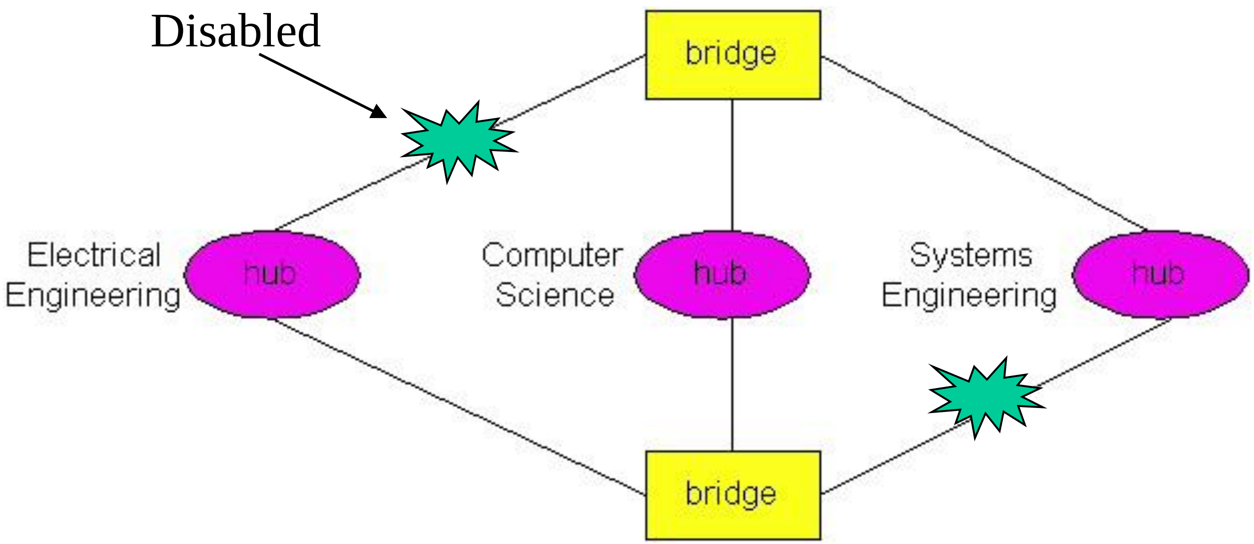
- Transparent bridges work fine as long as there are no redundant bridges in the system. Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable. If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable.

- 1. Station A sends a frame to station D. The tables of both bridges are empty. Both forward the frame and update their tables based on the source address A.
- 2. Now there are two copies of the frame on LAN 2. The copy sent out by bridge 1 is received by bridge 2, which does not have any information about the destination address D; it floods the bridge. The copy sent out by bridge 2 is received by bridge 1 and is sent out for lack of information about D. The tables of both bridges are updated, but still there is no information for destination D.

- 3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies flood the network.
- 4. The process continues on and on. Note that bridges are also repeaters and regenerate frames. So in each iteration, there are newly generated fresh copies of the frames.

Bridges Spanning Tree

- for increased reliability, desirable to have redundant, alternative paths from source to dest
- with multiple paths, cycles result - bridges may multiply and forward frame forever
- solution: organize bridges in a spanning tree by disabling subset of interfaces



Some bridge features

- Isolates collision domains resulting in higher total max throughput
- limitless number of nodes and geographical coverage
- Can connect different Ethernet types
- Transparent ("plug-and-play"): no configuration necessary

Bridges vs. Routers

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are link layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain bridge tables, implement filtering, learning and spanning tree algorithms